

## ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Review of the Update on Computer Security Legislation

FROM:

C/CSG/OIT

EXTENSION

NO

011 85-3861

DATE

5 DEC 1985

TO: (Officer designation, room number, and building)

DATE

RECEIVED

FORWARDED

OFFICER'S INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

1. DD/OIT-M  
2000 Has

11 Dec 85

[Signature]

2.

3.

OLL  
7B14- Hys

4.

5.

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

FORM 1-79

610

CONFIDENTIAL

1985

MEMORANDUM FOR: Deputy Director of Information Technology  
for Management

25X1 FROM:   
Computer Security Group, OIT

25X1 SUBJECT: Review of the Update on Computer Security  
Legislation

REFERENCE: Memo for Multiple fm LD/OLL, dtd 4 Nov 85,  
Subject: Update on Computer Security  
Legislation

25X1 1. The Computer Security Group (CSG) has reviewed the  
amended H.R. 2889 as provided by  in the reference  
memorandum. While it is not this Agency's intention to  
aggravate the House Government Operations Committee or any  
Branch of the Congress, I strongly believe that every attempt  
should be made to amend the Bill to preserve the authority of  
the DCI. Specifically, the Bill should include the language  
that was originally suggested that: "Nothing in this Bill  
alters the existing authorities of the Director of Central  
Intelligence, including his responsibility for the protection of  
intelligence sources and methods." Although this Agency may be  
exempt from Sections 3 and 4 of the Bill, by virtue of the  
Agency's exemption from the Federal Property and Administration  
Act of 1949, it is believed that the Agency should be  
25X1 specifically exempted from the entire Bill.

25X1 2. In reference to Section 5 of the Bill, CSG agrees with  
the original position, taken by the Agency, which states that the  
Agency must be able to continue its own strict Agency program in  
computer security. As long as the proposed Bill imposes minimum  
standards for training, this Agency's computer security training  
programs, which are more rigorous and stringent than other  
25X1 government agencies, should not be affected.

3. In reference to Section 6 of the Bill, CSG has serious  
concerns regarding the wording and intent of the proposed Bill.  
While it is true that a majority of the Agency's computer systems  
are classified, there are unclassified systems, specifically VMU,  
that would be affected by this Bill. Additionally, there are a



number of personal computers that are used throughout various Agency components in an "unclassified" mode. These systems, when taken in aggregate, could in fact become classified. The application of this Bill to "unclassified systems" was previously addressed by Donald C. Latham in his testimony before the Subcommittee on Legislation and National Security Committee on Government Operations, U.S. House of Representatives, on 18 September 1985. He suggested that the Bill be amended to read: "sensitive non-national security-related," as opposed to the proposed terminology in the Bill which states "sensitive but unclassified information." I support Mr. Latham's position and I also agree with Mr. Latham's statement that the Bill potentially could cause confusion, in that NSDD 145 has barely been in affect for 1 year. If H.R. 2889 is enacted, it is my opinion that it will only add to the confusion within the Federal Government regarding what standards and policies are to govern the Federal Government's computer systems since NSDD 145 establishes a mechanism under the National Telecommunications and Information Systems Security Committee for the promulgation of national computer security policies. [redacted]

4. While this Agency could let NSA, OMB, and NBS take the lead in opposing H.R. 2889, I believe it is in the Agency's best interest to lobby for a specific exclusion from this Bill to protect this Agency's equities. [redacted]



Washington, D.C. 20505

6 August 1985

Mr. James M. Frey  
Assistant Director for Legislative Reference  
Office of Management and Budget  
Washington, D.C. 20503

Dear Mr. Frey:

Enclosed is a response to a request by Congressman Brooks, Chairman of the House Government Operations Committee, for the views of the Agency on H.R. 2869, a bill to provide for computer security research and training of federal employees in computer security. The proposed response states that while we share the concern of the Congressman over computer security, the bill should be amended so as to allow the Agency to continue its own very strict mandatory training of personnel in computer security in accordance with established guidelines tailored to meet the security requirements of the Agency.

We ask that your office review the Agency's response and advise us as to whether or not there is an objection to its transmittal. Since Congressman Brooks has requested a prompt reply, we would appreciate expedited action on our response.

Sincerely,



Charles A. Briggs  
Director, Office of Legislative Liaison

Enclosure

25X1

Central Intelligence Agency



Washington, D.C. 20505

The Honorable Jack Brooks  
Chairman  
Committee on Government Operations  
House of Representatives  
Washington, D.C. 20515

Dear Mr. Chairman:

This letter is in response to your request for the views of the Central Intelligence Agency on H.R. 2889, a bill introduced by Congressman Glickman to provide for a computer security research program and training of federal employees who are involved in the management, operation, and use of computers. Mr. Casey has asked me to respond on his behalf. While the Agency agrees with the congressional findings in the bill regarding the need to train employees in computer security procedures, we believe the bill should be amended to preserve the authority of the Director to continue the Agency's own very strict computer security program in accordance with established guidelines.

There is little doubt that the Federal Government needs to improve the security of its computers. Computers now store a very large amount of highly classified data and sensitive information and have become a target for hostile foreign powers engaged in espionage. Should a foreign power gain access to this Agency's computers or those of agencies of the Intelligence Community, the harm to national security would be extraordinary. In addition to the threat from hostile intelligence services, the Agency must also be mindful of the threat posed by the so called "hackers" who illegally break into government computers.

The Agency has a very active program underway to safeguard its computers from unauthorized access. This program includes the procuring of both hardware and software designed to ensure the highest degree of security. There is also a research program underway designed to create new systems capable of defeating the most determined and sophisticated means of accessing our computers without authorization. Finally, we conduct a very rigorous program to educate our employees on

computer security awareness and good security practice. We believe this program has been highly successful in safeguarding our information.

Should the Government Operations Committee decide to go forward on this legislation, we believe that the bill should be amended to preserve the authority of DCI to safeguard Agency computers against unauthorized access. Specifically, we suggest that the following language be inserted into the Bill:

Nothing in this bill alters the existing authorities of the Director of Central Intelligence, including his responsibility for the protection of intelligence sources and methods.

Adding this language to the bill will ensure that the Agency will be able to continue its own very strict mandatory training of personnel in computer security in accordance with established guidelines tailored to meet the security requirements of the Agency. [This mandatory computer security program is more stringent than other agencies that do not regularly deal in classified information.] A single set of regulations to cover all federal agencies that does not accommodate the particular security needs of individual agencies is not the most effective means to provide the necessary protection needed for computers containing our nation's most sensitive secrets.

We appreciate the opportunity to comment on this legislation. If you or your staff have any questions on our comments on this bill, please do not hesitate to contact me or

STAT

The Office of Management and Budget has advised that there is no objection to the submission of this report from the standpoint of the Administration's program.

Sincerely,

Charles A. Briggs  
Director, Office of Legislative Liaison

OLL85-2723/1  
16 September 1985

MEMORANDUM FOR: Director, Office of Security  
✓ Deputy Director, Office Information Technology  
Chief, ILD/OGC

STAT

FROM:   
Chief, Legislation Division/OLL

SUBJECT: Request for Comments on DOD Testimony on  
H.R. 2889, Computer Security Research and  
Training Act of 1985

1. Attached for your review and comment is DOD's testimony on H.R. 2889, the Computer Security Research and Training Act of 1985. This bill, also attached, provides for the National Bureau of Standards (NBS) to establish a computer security research program to address the problem of computer security in the Federal government. The bill also requires each federal agency to furnish mandatory periodic training in computer security for all employees who are involved with the management, use or operation of computers or other automated information systems.

2. In the attached testimony, DOD endorses the general intent of H.R. 2889, but requests that this legislation more carefully delineate the exact scope of NBS's charter in developing standards in this area. Specifically, DOD suggests that NBS' responsibilities be limited to establishing programs which address "unclassified but sensitive non-national security-related information". NSDD 145 would continue to apply to classified national security information. While DOD notes that H.R. 2889 and NSDD 145 address two different categories of information, the attached testimony does strongly emphasize the need for continued cooperation between NBS' efforts and that of DOD and other national security agencies in this area.

3. OMB requires our comments on the attached testimony by noon Tuesday, 17 September 1985. I apologize for this short deadline, but this office did not receive this testimony until 5 o'clock today.

STAT

Attachments  
as stated



**STATEMENT**

**BY**

**DONALD C. LATHAM**

**ASSISTANT SECRETARY OF DEFENSE**

**COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE**

**AND**

**CHAIRMAN**

**NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY**

**COMMITTEE**

**CONCERNING H.R. 2889**

**BEFORE THE**

**SUBCOMMITTEE**

**ON LEGISLATION AND NATIONAL SECURITY**

**COMMITTEE ON GOVERNMENT OPERATIONS**

**UNITED STATES HOUSE OF REPRESENTATIVES**

**SEPTEMBER 18, 1985**



Mr. Chairman and members of the Subcommittee:

Thank you for this opportunity to testify on H.R. 2889, known as the "Computer Security Research and Training Act of 1985". This bill has the objectives of providing for a computer security research program within the National Bureau of Standards (NBS) and also providing for the training of Federal Employees who are involved in the management, operation, and use of automated information (AIS) systems. The efforts of this subcommittee are to be applauded as it carries out in its investigation of the importance of the computer systems security problem to this nation and considers actions aimed at coming up with comprehensive remedies to this complex issue.

Today, I would like to address myself first to the general intent and overall purpose of the bill by providing perspectives, in my dual roles as both the Assistant Secretary of Defense for Command, Control and Communications and Chairman, National Telecommunications and Information Systems Security Committee (NTISSC), of the problems we face. Second, I would like to highlight possible areas of potential confusion in the bill requiring clarification so as not to impact adversely on existing Administration programs. Finally, I have included in my testimony suggested revisions to the bill for your careful review and action.

First, I wholeheartedly support the general intent of H.R. 2889 to provide for much needed support in the area of computer systems security training and education. All too often this is an area sorely overlooked and poorly funded because it is not glamorous. Also, as you are all too aware, the computer system security problem is extremely complex and solutions to the problem are made all the more difficult by continuing rapid advances in the state-of-the-art. The emerging use of supercomputers and the proliferation of local area networks are but two examples of technology that make the computer systems security problem a challenge that must be faced now. The problem is immense in scope and associated R&D in the area is totally inadequate. The shortage of highly qualified and trained professionals in computer systems security aggravates the problem. Any effort to try to assist in this endeavor is clearly welcome.

In this regard, I view H.R. 2889 as a positive step to achieve consensus on the need for additional resources. The National Bureau of Standards has for some time been an important center of expertise in certain facets of computer systems security. It is entirely appropriate, therefore, that the NBS be tapped to take on additional responsibilities and funding in research and related activities as reiterated in the Bill. Let me quickly caveat my comments by saying that, to be truly effective, these additional NBS efforts must be further focused in the context of on-going efforts such as those which fall under National Security Decision Directive (NSDD-145) so to avoid costly duplication of effort. I will address this issue in some detail later.

As Chairman of the NTISSC, I view as one of my key responsibilities making sure the problem of computer systems security is recognized by the public at-large as an important national issue. We have not done as good a job as we might have done in the past because we were not properly organized. The NTISSC structure now in being provides that organization and we are moving ahead with an aggressive awareness program in concert with similar initiatives being carried out by the NBS.

At its last meeting on 4 September 1985, the Subcommittee on Automated Information Systems security (SAISS), one of the two major subcommittees of the NTISSC, approved for issuance to the NTISSC a proposal to require education and training of federal departments and agencies. I expect the NTISSC to take up this proposal and make it a National Policy. In this regard, the National Computer Security Center (NCSC) at the National Security Agency (NSA) has begun development of training courses in AIS systems security for a DoD-sponsored awareness program. The NCSC will provide materials to other government, departments and agencies for awareness training. Of course, funding for such training resources remains a problem.

Let me focus just a moment on some other DoD education and training efforts. We are developing guidelines which will make it easier to determine and specify the level of security that a system needs when generating requests for procurements or acquisitions. Also, we are in the process of issuing a Standard entitled, "DoD Trusted Computer System Evaluation Criteria", hereafter referred to as the Criteria, to assist in evaluating the effectiveness of safeguards for Defense applications. By the way, the SAISS adopted use of the Criteria on an interim one-year trial basis. Finally, the DoD is undertaking an ambitious computer vulnerability reporting program aimed at correcting security weaknesses in DoD computer systems. This effort should also be very useful for designing a national reporting program.

In my testimony for Mr. Glickman, Chairman of the Subcommittee on Transportation, Aviation and Materials, Committee on Science and Technology, on 27 June 1985, I indicated that a high priority item was trying to provide a working definition for what constitutes "sensitive" information. Since that time, the SAISS has approved for issuance to the NTISSC a proposal for defining sensitive information. Specifically, it separates unclassified but sensitive information into two categories: sensitive national security-related and sensitive non-national security-related. The purview of NSDD 145 is only for the former category. Unclassified but sensitive non-national security-related is the concern of the civilian sector with NBS playing a major role.

Let me reiterate that NSDD-145 does not cover unclassified but sensitive non-national security-related information and therefore, it in no way restricts, controls, or manages the activities of other federal departments or agencies who have responsibilities in non-national security-related areas. In order to maintain this clear

demarcation line, language in H.R. 2889 making reference to "sensitive" information should be amended to reflect that "unclassified but sensitive non-national security-related" data is the subject data in question.

On the matter of research and development (R&D) responsibilities, the NBS has a well-developed program in the area of computer systems security. The NBS derives its responsibilities from the Brooks Act of 1965 (P.L. 89-306), the Privacy Act of 1974 (P.L. 93-579), and the Paperwork Reduction Act of 1980 (P.L. 96-511). We view these responsibilities as distinct both in intent and focus from those cited in NSDD-145. Again, NSDD-145 addresses only unclassified but sensitive national security-related and does not cover unclassified but sensitive non-national security-related information. More directly, privacy information, information on fraud, waste, and abuse, or proprietary data held by an agency is not covered by NSDD-145 dictates.

Let me quickly add that we don't intend to meddle in NBS authorities or responsibilities in these areas. Rather, we see the NBS efforts and those of other federal agencies under NSDD-145 as complementary and supportive of each other. Clearly, technical measures and techniques can apply equally well in many circumstances and technical interaction must be encouraged.

Indicative of the strong current relationship between the NBS and the DoD, is the high-level of cooperation between the NBS and the National Computer Security Center at NSA which is already impressive and growing. Specifically, they have jointly sponsored for the past eight years a National Computer Security Conference. This year's conference, scheduled from 29 September 1985 to 3 October 1985, will focus on mutual subjects of concern such as secure networks, verification, labelling, a profile of "hackers", and data base management security to name just a few. It will be attended by business, academia and government and allows for critical transfer of the results of the National Computer Security Center research and the NBS research throughout government and the private sector.

Important work is proceeding between NBS and the NCSC in the area of personal computers and office automation. In this regard, a Guideline on Password Management is being published by the NCSC and will become an appendix to the NBS Password Usage Standard already in existence. Additionally, the NBS has done impressive work in micro-computer and mini-computer systems security which the NCSC is using. As a final example, NBS and the NCSC is sponsoring a symposium on risk analysis to examine methodologies of mutual benefit. Again, these efforts represent the high degree of interaction between these two centers of expertise.

This cooperation must continue. However, the federal audiences for their respective services is different. The NCSC's target audience is the National Security Community while NBS services the

civilian sector. While the staffs of both organizations are highly specialized, there is continuing reliance by NCSC staff on NBS Institute for Computer Sciences and Technology (ICST) staff expertise and vice-versa. In fact, two NSA employees currently are working at NBS with the purpose of transferring expertise to civilian users. This arrangement has worked remarkably well in the past and must be preserved.

Let me add that the NBS has taken an active role in the Subcommittee on Automated Information Systems Security (SAISS) of the NTISSC. The NBS member is the ICST Director, Mr. James Burrows. Mr. Burrows has been instrumental in the promulgation by the SAISS of the recent issuance relating to defining sensitive information categories as well as the issuance on training and education.

As a final point on the issue of NSDD-145 and NBS responsibilities, NSDD-145 requires that NBS submit for NTISSC approval proposed computer systems security standards prior to their issuance as a Federal Information Processing System (FIPS) standard. Once again, this applies only to proposed standards where national security-related matters are concerned. Standards unrelated to national security are not covered. In this regard, it is anticipated that, Federal Information Processing Standard No. 112, Password Usage Standards, will be the first such standard processed under the NTISSC structure because it has application to both unclassified and classified processing environments.

In accordance with the preceding, I would now like to turn my attention to some of the areas in the bill that potentially could cause confusion and which, I feel, could benefit from additional clarification.

First, on page 2 of H.R. 2889, reference is made to "sensitive" information. I suggest this be amended to read "sensitive unclassified non-national security-related." Also, for clarity, this phrase should also be used to modify the use of the term "information" as used on page 3 Sec. 18 (b) (2).

Second, on page 3 of H.R. 2889, Section 18 (a) should be amended to clearly set forth that H.R. 2889 does not seek to impact Administration efforts under NSDD-145. Therefore, I propose the following be inserted as the last sentence of paragraph (c): "The following NBS program shall be undertaken in consonance with those computer system security responsibilities delineated in National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information System Security." This important adjustment minimizes overlap of responsibilities between the Department of Commerce and the Department of Defense and recognizes that both programs are complementary and supportive.

In closing, let me allay the fears of those who feel that NSDD-145 does in some way, shape, or form restrict current NBS

Research and development for standards-making efforts. NSDD-145 and the NBS programs stemming from the statutory base already mentioned are compatible and complementary efforts.

Computer systems security is a major challenge that needs all the available brainpower and resources this nation can muster. As such, let's move ahead together in the spirit of harmony and cooperation, not competition. I feel H.R. 2889, with the recommended changes I proposed, is a positive step in fostering this spirit of cooperation.

Accompanying me is Mr. Robert Rich, Deputy Director, NSA, who will further describe the activities of the Computer Security Center and other programs now being carried out by NSA in the areas of computer systems security awareness, education, training, and research and development.

Mr. Chairman, this concludes my prepared remarks. I would be happy to answer any questions that you or the Subcommittee have.

99TH CONGRESS  
1ST SESSION

# H. R. 2889

To amend the Act establishing the National Bureau of Standards to provide for a computer security research program within such Bureau, and to provide for the training of Federal employees who are involved in the management, operation, and use of automated information processing systems.

## IN THE HOUSE OF REPRESENTATIVES

JUNE 27, 1985

Mr. GLICKMAN (for himself, Mr. FUQUA, Mr. BROOKS, Mr. BROWN of California, Mr. WIRTH, Mr. WALGREN, Mr. NELSON of Florida, Mr. WYDEN, Mr. HUGHES, Mr. LEWIS of Florida, and Mr. HORTON) introduced the following bill; which was referred jointly to the Committees on Science and Technology and Government Operations

## A BILL

To amend the Act establishing the National Bureau of Standards to provide for a computer security research program within such Bureau, and to provide for the training of Federal employees who are involved in the management, operation, and use of automated information processing systems.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled.*

### 3 SECTION 1. SHORT TITLE.

4 This Act may be cited as the "Computer Security  
5 Research and Training Act of 1985".

## 1 SEC. 2. FINDINGS.

2 The Congress finds that—

3 (1) in recent years the Federal Government has  
4 become highly dependent on automated information  
5 processing systems for carrying out many of its  
6 missions.

7 (2) the Government operates about 20,000  
8 medium- and large-scale mainframe computers, and by  
9 the end of this decade it will also have approximately  
10 half a million micro- and mini-computers;

11 (3) the information stored in Government comput-  
12 ers and transmitted over the various communications  
13 networks that connect them represent valued property  
14 that is vulnerable to unauthorized access and disclo-  
15 sure, fraudulent manipulation, and disruption;

16 (4) studies of computer-related fraud and abuse in  
17 Government agencies indicate a costly and widespread  
18 problem of significant proportions;

19 (5) Government efforts to address the problems of  
20 computer security have focused on developing hard-  
21 ware and software systems to protect sensitive infor-  
22 mation, ensuring that new computer systems are de-  
23 signed to include security provisions, and requiring  
24 agencies to implement security procedures; and

25 (6) the existing law must be supplemented if the prob-

1 the information stored, processed, and transmitted by  
2 Government computers remains the people who  
3 manage, use, and operate them.

4 SEC. 3. ESTABLISHMENT OF COMPUTER SECURITY RESEARCH  
5 PROGRAM.

6 The Act of March 3, 1901 (15 U.S.C. 271-273), is  
7 amended by redesignating section 18 as section 19, and by  
8 inserting after section 17 the following new section:

9 "SEC. 18. (a) The National Bureau of Standards shall  
10 establish and conduct a computer security research program  
11 to address the problems of computer security in the Federal  
12 Government, with primary emphasis upon the prevention of  
13 computer-related fraud and abuse through the training of em-  
14 ployees in computer security awareness and good security  
15 practice.

16 "(b) The program shall—

17 "(1) perform research and conduct studies to de-  
18 termine the nature and extent of computer security  
19 vulnerability in Federal agencies and their contractors;

20 "(2) devise administrative, management, and tech-  
21 nical procedures and practices designed to protect the  
22 information stored, processed, and transmitted by  
23 Government computers; and

24 "(3) develop guidelines for use by Federal agen-  
25 cies in training their employees, and the employees of





1       (c) **REGULATIONS.**— Within six months after the date of  
2 the enactment of this Act, the Director of the Office of Per-  
3 sonnel Management shall issue regulations prescribing in  
4 detail the procedures and scope of the training to be provided  
5 by Federal agencies under subsection (a) and the manner in  
6 which such training is to be carried out.

7 **SEC. 5. AUTHORIZATION OF APPROPRIATIONS.**

8       There are hereby authorized to be appropriated to the  
9 National Bureau of Standards for the fiscal year 1987, to  
10 carry out the computer security research program under sec-  
11 tion 18 of the Act of March 3, 1901 (as added by section 3 of  
12 this Act), such sums as may be necessary.

○

OLL 85-3400  
4 November 1985

MEMORANDUM FOR: Director, Office of Security  
Chief, Legislative Liaison, IC Staff  
Deputy Director, Office of Information &  
Technology Management

STAT

FROM: [REDACTED]  
Legislation Division  
Office of Legislative Liaison

SUBJECT: Update on Computer Security Legislation

STAT

REFERENCE: Memo to Director, Office of Security, from  
[REDACTED] dated 16 July 1985, same subject

1. The purpose of this memo is to provide an update on the status of H.R. 2889, the Computer Security Act of 1985. You may recall that this legislation was introduced by Representatives Glickman and Brooks on 27 June and referred jointly to the House Committees on Science and Technology and Government Operations. As originally introduced, the bill provided that the National Bureau of Standards shall establish and conduct a computer security research program for the federal government and develop guidelines for use by federal agencies in training their employees in computer security awareness and good security practices. The bill also provided that the details and scope of the training would be prescribed by OMB.

2. In response to a request by Congressman Brooks, we sent a letter on 19 September 1985 to the Congressman containing our views on the legislation. The letter endorsed the goal of the bill, i.e., improving computer security, but requested that the bill be amended to preserve the authority of the DCI to safeguard Agency computers. Following hearings held on 18 September 1985, the Subcommittee on Legislation and National Security of the House Government Operations Committee on 23 October conducted a markup of H.R. 2889. In the markup, an amendment in the nature of a substitute was offered by Congressman Brooks and was adopted by the Subcommittee. A copy of the amendment is attached. On 29 October the full House Government Operations Committee approved the bill.

3. Although H.R. 2889 as approved by the Government Operations Committee did not incorporate our suggested amendment, I believe that the amended bill substantially benefits the Agency by excluding the Agency from most of its provisions. [Section 3] of the bill would give the National Bureau of Standards (NBS) sole jurisdiction over the computer security issue in the federal government, but only to the extent the computer and telecommunication systems are subject to the provisions of section 111 of the Federal Property and Administration Act of 1949 (40 USC §759) or chapter 35 of Title 44. The Agency is exempt from the Federal Property and Administration Act by virtue of 40 U.S.C. §474 (17). The Agency is exempt from the provisions of chapter 35 of Title 44, U.S.C., that pertain to computer and telecommunication systems by virtue of 44 U.S.C. §3502. Thus the provisions of section 3 of the bill would not apply to the Agency. The Agency is also exempt from [section 4] of the bill, which pertains to the establishment of automatic data processing and related telecommunications standards, because this section amends the Federal Property and Administration Act. \*

4. The Agency probably would not be exempt from Section 5 of the bill, which requires periodic mandatory training of its personnel in computer security in accordance with regulations issued by OPM.<sup>1</sup> I have discussed with congressional staff the Agency's concern that these regulations would establish training guidelines that would not be sufficient for own security needs. The staff has stated that these guidelines would only establish minimum training standards and that an agency would be free to establish more rigorous training to protect computers that contain highly classified data. In

---

<sup>1</sup>An argument could be made that this section does not apply to the Agency since these regulations are to be developed in accordance with section 3 of the Act, which the Agency is exempt from. I am not prepared at this point, however, to certify that such an argument would carry the day.

Distribution:

Original - Addressees

1 - D/OLL

1 - DD/OLL

1 - OLL Chrono

1 - Leg/Sub - Computer Fraud

1 - DMP Signer

STAT LEG/OLL:  (4 November 1985)

addition, you should be aware that OPM on 30 October testified before a subcommittee of the House Science and Technology Committee that this legislative authority was unnecessary and that agency heads should be given some discretion in setting up their training programs. Congressman Glickman agreed with this and stated that provision may be changed.

5. The Agency is also not exempt from section 6 of the bill, which requires that each federal agency identify computer and telecommunication equipment systems that store unclassified but sensitive data. The section also requires that the federal agency establish a plan for the security of those computers storing unclassified data and that such plans be transmitted to NBS and NSA and be subject to disapproval by GSA. I suspect that the impact on us would not be great since our computer systems store mostly classified information. ?

6. It is my judgment that this legislation will move forward in the House during the next month. The House Science and Technology Committee has completed its hearings on this matter and will markup the legislation in the next few weeks. During these hearings, held on 29 and 30 October, the Administration came out forcefully against the bill. NSA and OPM both stated that the legislation was not necessary and would do more harm than good. More significantly, James Burrow, the Director for the Institute of Computer Science and Technology, NBS, has come out strongly against the bill, as has the Deputy Secretary of Commerce. Despite this opposition, Congressman Brooks is determined to move this legislation forward and the bill will probably pass the House before the end of the year. Prospects for Senate action remain uncertain.

7. Because the legislation will be moving forward, it is necessary that the Agency make a determination whether to take an active role in opposing the bill or amending it further. I would appreciate your review of Sections 5 and 6 of the bill to determine whether these sections would cause significant problems for the Agency. My inclination is to let NSA, OMB, and NBS take the lead in opposing the legislation. If you believe that further amendments to the legislation are in order to protect Agency equities, please let me know so that we can take appropriate action.

STAT



Attachment:  
as stated

BROOKS284

AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 2889  
OFFERED BY MR. BROOKS

Strike out all after the enacting clause and insert in  
lieu thereof the following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the ``Computer Security Act of  
3 1985``.

4 SEC. 2. FINDINGS.

5 The Congress finds that--

6 (1) in recent years the Federal Government has become  
7 highly dependent on automated information processing  
8 systems for carrying out many of its missions;

9 (2) the Government operates about 20,000 medium- and  
10 large-scale mainframe computers and by the end of this  
11 decade it will also have approximately half a million  
12 micro- and mini-computers;

13 (3) the information stored in Government computers  
14 and transmitted over the various communications networks  
15 that connect them represent valued property that is  
16 vulnerable to unauthorized access and disclosure,  
17 fraudulent manipulation, and disruption;

18 (4) studies of computer-related fraud and abuse in  
19 Government agencies indicate a costly and widespread

BROOKS284

2

1 problem of significant proportions;

2 (5) Government efforts to address the problems of  
3 computer security have focused on developing hardware and  
4 software systems to protect sensitive information,  
5 ensuring that new computer systems are designed to  
6 include security provisions, and requiring agencies to  
7 implement security procedures; and

8 (6) these efforts must be supplemented if the  
9 problems are to be solved, since the weak link in  
10 protecting the information stored, processed, and  
11 transmitted by Government computers remains the people  
12 who manage, use and operate them.

13 SEC. 3. ESTABLISHMENT OF COMPUTER SECURITY MANAGEMENT, *EXEMPT*  
14 RESEARCH, AND TRAINING PROGRAM.

15 The Act of March 3, 1901 (15 U.S.C. 271-278h), is amended  
16 by redesignating section 18 as section 20, and by inserting  
17 after section 17 the following new sections:

18 SEC. 18. (a) The National Bureau of Standards shall  
19 have the sole authority and responsibility for establishing  
20 and conducting a computer security management, research, and  
21 training program pertaining to computer and  
22 telecommunications systems that are subject to the provisions  
23 of section 111 of the Federal Property and Administrative  
24 Services Act of 1949 (40 U.S.C. 759) or chapter 35 of title  
25 44, United States Code. The primary emphasis of such program



BR008184

3

1 shall be the prevention of computer-related fraud and abuse.  
2 For such purpose, the Bureau shall prepare and submit to the  
3 Secretary of Commerce, for promulgation under such section  
4 111, government-wide standards and guidelines.

5 `` (b) In carrying out the program described in subsection  
6 (a), the Bureau shall--

7 `` (1) perform research and conduct studies to  
8 determine the nature and extent of computer and  
9 telecommunications systems vulnerabilities in Federal  
10 agencies and their contractors;

11 `` (2) devise management, administrative, technical,  
12 and physical procedures and practices designed to protect  
13 the information stored, processed, and transmitted by  
14 Government computer and telecommunications systems;

15 `` (3) develop standards and guidelines and offer  
16 assistance for use by Federal agencies in training their  
17 employees, and the employees of their contractors and of  
18 other organizations whose computer or telecommunications  
19 systems interface with Government computer systems, in  
20 computer and telecommunications security awareness and  
21 accepted security practices;

22 `` (4) make recommendations to the General Services  
23 Administration on computer and telecommunications  
24 security policy and on revisions of regulations proposed  
25 pursuant to section 111(f)(3) of the Federal Property and

BOOKS 284

Administrative Services Act of 1949;

(5) develop and coordinate, as appropriate, with the General Services Administration, the Office of Personnel Management, and the National Security Agency, joint computer and telecommunications security standards, research, and training programs; and

NSDD 145

(6) investigate compliance with computer and telecommunications security standards through research, inspection, and reporting activities;

(7) act as liaison between the Federal Government and the private sector with respect to computer and telecommunications security issues involving sensitive but unclassified information and assist the private sector in using and applying the results of the programs and activities under this section; and

(8) establish an advisory council composed of representatives of other Federal agencies.

SEC. 19. (a) There is hereby established a Computer and Telecommunications Privacy and Security Advisory Board within the National Bureau of Standards. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

(1) four members from outside the Federal Government who are eminent in the computer or

BROOKING

5

1 telecommunications industry, at least one of whom shall  
2 be from a small or medium sized company in such industry;

3       “(2) four members from outside the Federal  
4 Government who are eminent in the fields of computer or  
5 telecommunications technology, or related disciplines,  
6 but who are not employed by a producer of computer or  
7 telecommunications equipment; and

8       “(3) four members from the Federal Government who  
9 have computer or telecommunications systems management  
10 experience, including experience in computer security or  
11 telecommunications security, at least one of whom shall  
12 be from the National Security Agency.

13       “(b) The duties of the Board shall be--

14       “(1) to identify emerging managerial, technical  
15 administrative, and physical safeguard issues relative to  
16 computer and telecommunications systems security; and

17       “(2) to advise the Bureau of Standards and the  
18 Secretary of Commerce on security and privacy issues  
19 pertaining to computer and telecommunications systems of  
20 the Federal Government.

21       “(c) The term of office of each member of the Board  
22 shall be four years, except that--

23       “(1) of the initial members, three shall be  
24 appointed for terms of one year, three shall be appointed  
25 for terms of two years, three shall be appointed for

1 terms of three years, and three shall be appointed for  
2 terms of four years; and

3 "(2) any member appointed to fill a vacancy in the  
4 Board shall serve for the remainder of the term for which  
5 his predecessor was appointed.

6 "(d) The Board shall not act in the absence of a quorum,  
7 which shall consist of seven members. Members of the Board,  
8 other than full-time employees of the Federal Government, may  
9 be compensated at a rate not to exceed the maximum rate of  
10 pay for grade GS-18, as provided in subchapter III of chapter  
11 53, title 5, United States Code, when engaged in the actual  
12 performance of duties vested in the Board.

13 "(e) Members of the Board, other than full-time  
14 employees of the Federal Government, while attending meetings  
15 of such committees or while otherwise performing duties at  
16 the request of the Board Chairman while away from their homes  
17 or a regular place of business, may be allowed travel  
18 expenses in accordance with subchapter I of chapter 57 of  
19 title 5, United States Code.

20 "(f) To provide the staff services necessary to assist  
21 the Board in carrying out its functions, the Board may  
22 utilize personnel from the National Bureau of Standards or  
23 any other agency of the Federal Government with the consent  
24 of the head of the agency."

25 SEC. 4. AMENDMENT TO BROOKS ACT.

1 Section 111(f) of the Federal Property and Administrative  
2 Services Act of 1949 (40 U.S.C. 759(f)) is amended to read as  
3 follows:

4 "(f)(1) The Secretary of Commerce shall--

5 "(A) provide agencies, and the Administrator in  
6 the exercise of functions delegated in this section,  
7 with scientific and technological advisory services  
8 relating to automatic data processing and related  
9 systems, including telecommunications systems;

10 "(B) establish uniform Federal automatic data  
11 processing and related telecommunications standards  
12 and guidelines; and

13 "(C) on the basis of standards and guidelines  
14 developed by the National Bureau of Standards  
15 pursuant to section 18(b)(3) of the Act of March 3,  
16 1901 (15 U.S.C. 271 et seq.), establish standards and  
17 guidelines for the security of computer and  
18 telecommunications systems that are subject to this  
19 section.

20 "(2) The standards established by the Secretary of  
21 Commerce under paragraphs (1)(B) and (1)(C) shall be  
22 compulsory and binding on each Federal agency unless waived  
23 by the Secretary of Commerce in writing upon a determination  
24 that compliance would adversely affect the accomplishment of  
25 the agency's mission or cause a major adverse financial

1 impact on the agency which is not offset by government-wide  
2 savings. Notice of each such waiver shall be promptly  
3 transmitted to the Committee on Government Operations of the  
4 House of Representatives and the Committee on Governmental  
5 Affairs of the Senate.

6       “(3) The Administrator shall ensure that such standards  
7 and guidelines are implemented within an integrated  
8 information resources management system (as required by  
9 chapter 35 of title 44, United States Code) by--

10           “(A) developing and implementing policies on  
11 automatic data processing and related telecommunications  
12 systems security; and

13           “(B) revising the Federal information resources  
14 management regulations (41 CFR ch. 201) consistent with  
15 such standards, guidelines, and policies.

16       “(4) In carrying out functions under paragraph (1) of  
17 this subsection, the Secretary of Commerce and the Director  
18 of the National Bureau of Standards are authorized--

19           “(A) to accept, hold, administer, and use gifts and  
20 bequests of property, both real and personal, for the  
21 purpose of aiding or facilitating such functions; and

22           “(B) to accept reimbursement for the performance of  
23 such functions for the benefit of another Federal agency  
24 or for the benefit of any other person or organization,  
25 at rates approximating the costs thereof.

1       “(5) The Secretary is authorized to undertake the  
2 necessary research in the sciences and technologies of  
3 automatic data processing computer and related systems,  
4 including telecommunications systems, as may be required  
5 under the provisions of this subsection.”.

6       SEC. 5. TRAINING BY FEDERAL AGENCIES IN COMPUTER AND  
7                       TELECOMMUNICATIONS SECURITY.

8       (a) IN GENERAL.--Each Federal agency (as that term is  
9 defined in section 3(b) of the Federal Property and  
10 Administrative Services Act of 1949) shall provide mandatory  
11 periodic training in computer and telecommunications  
12 security. Such training shall be provided under the  
13 guidelines developed pursuant to section 18(b)(3) of the Act  
14 of March 3, 1901 (as added by section 3 of this Act), and in  
15 accordance with the regulations issued under subsection (c)  
16 of this section, for all of the agency's employees who are  
17 involved with the management, use, or operation of computer  
18 or other automated information systems, including related  
19 telecommunications systems, and for all of the employees and  
20 other personnel of its contractors who are involved with the  
21 management, use, or operation of computers which interface  
22 with Government systems.

23       (b) TRAINING OBJECTIVES.--Training under this section  
24 shall be started within 60 days after the issuance of the  
25 regulations described in subsection (c). Such training shall

1 be designed--

2 (1) to enhance employees' awareness of the threats to  
3 and vulnerability of computer and telecommunications  
4 systems; and

5 (2) to encourage the use of improved computer  
6 security practices at Government facilities.

7 (c) REGULATIONS.--Within six months after the date of the  
8 enactment of this Act, the Director of the Office of  
9 Personnel Management shall issue regulations prescribing in  
10 detail the procedures and scope of the training to be  
11 provided by Federal agencies under subsection (a) and the  
12 manner in which such training is to be carried out.

13 SEC. 6. ADDITIONAL FEDERAL AGENCY RESPONSIBILITIES FOR \*  
14 COMPUTER AND TELECOMMUNICATIONS SECURITY.

15 (a) IDENTIFICATION OF SENSITIVE SYSTEMS.--Within 6 months  
16 after the date of enactment of this Act, each Federal agency  
17 (as that term is defined in section 3(b) of the Federal  
18 Property and Administrative Services Act of 1949) shall  
19 identify each computer and related telecommunications system  
20 of that agency within which is or will be stored or through  
21 which is or will be transmitted sensitive (but unclassified)  
22 information the loss or misuse of which could adversely  
23 affect the national interest or the conduct of Federal  
24 programs.

25 (b) SECURITY PLAN.--Within one year after the date of



BROOKS 284

11

1 enactment of this Act, each such Federal agency shall,  
2 consistent with the standards, guidelines, policies, and  
3 regulations prescribed pursuant to section 111(f) of the  
4 Federal Property and Administrative Services Act of 1949,  
5 establish a plan for the security of the computer and related  
6 telecommunications systems and systems in development  
7 identified pursuant to subsection (a). Copies of such plan  
8 shall be transmitted to the National Bureau of Standards and  
9 the National Security Agency for advice and comment. Such  
10 plan shall be subject to disapproval by the Administrator of  
11 General Services.

12 **SEC. 7. AUTHORIZATION OF APPROPRIATIONS.**

13 There are hereby authorized to be appropriated to the  
14 National Bureau of Standards for the fiscal years 1987, 1988,  
15 and 1989 to carry out the computer security management,  
16 research, and training program established by this Act, such  
17 sums as may be necessary. There are also authorized to be  
18 appropriated to each Federal agency such sums as may be  
19 necessary for fiscal years 1987, 1988, and 1989 to carry out  
20 the computer and telecommunications security training program  
21 established by section 5 of this Act and the identification  
22 and planning requirement of section 6.